

# PERSONAL DATA PROTECTION ACT

*In force as from 1 January 2002*

*Promulgated, State Gazette (SG) No 1 of 4 January 2002, amended SG No 70 of 10 August 2004, amended SG No 93 of 19 October 2004, amended SG No 43 of 20 May 2005, amended SG No 103 of 23 December 2005, amended SG No 30 of 11 April 2006, amended SG No 91 of 10 November 2006, amended SG No 57 of 13 July 2007, amended SG No 42 of 5 June 2009, amended SG No 94 of 30 November 2010, amended SG No 97 of 10 December 2010, amended SG No 39 of 20 May 2011, amended SG No 81 of 18 October 2011, amended SG No 105 of 29 December 2011, amended and supplemented SG No 15 of 15 February 2013, supplemented SG No 81 of 14 October 2016, amended SG No 85 of 24 October 2017, supplemented SG No 103 of 28 December 2017, amended SG No 7 of 19 January 2018, amended and supplemented SG No 17 of 26 February 2019, amended SG No 93 of 26 November 2019, amended SG No 93 of 26 November 2019, **amended and supplemented SG. 11/2 Feb 2023***

## Chapter One GENERAL PROVISIONS

Article 1. (Amended, SG No 103 of 2005, amended, SG No 17 of 2019) (1) This Act governs the social relations in connection with the protection of natural persons with regard to processing of personal data, as long as they are not regulated by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1 of 4 May 2016), hereinafter referred to as “Regulation (EU) 2016/679”.

(2) This Act lays down rules with regard to the protection of natural persons with regards to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats to public order and security.

(3) The purpose of this Act is to ensure protection of natural persons with regard to the processing of personal data in accordance with Regulation (EU) 2016/679, as well as the processing of personal data by the competent authorities for the purposes referred to in Paragraph (2).

(4) This Act furthermore governs:

1. the status of the Commission for Personal Data Protection as a supervisory authority responsible for the protection of the fundamental rights and freedoms of natural persons with regard to processing and facilitation of the free flow of personal data within the European Union;

2. the powers of the Inspectorate of the Supreme Judicial Council in the exercise of supervision regarding the processing of personal data in the cases referred to in Article 17;

3. the remedies;
4. accreditation and certification in the field of personal data protection;
5. specific data processing cases.

(5) This Act shall not apply to the processing of personal data for the purposes of national defence and national security unless otherwise provided in a specific law.

(6) This Act shall not apply to the processing of personal data of deceased persons, except in the cases referred to in Article 25f.

(7) Pursuant to the processing of personal data under Article 2 of Regulation (EU) 2016/679, the States which are Contracting Parties to the Agreement on the European Economic Area and the Swiss Confederation shall have the same status as the Member States of the European Union. All other States shall be third countries.

(8) When data is processed for the purposes referred to in Article 42 (1), the States that implement, apply and develop the Schengen *acquis* shall have the same status as the Member States of the European Union. All other States shall be third countries.

Article 2. (Supplemented, SG No 70 of 2004, in force as from 1 January 2005, amended, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 3. (Repealed, SG No 17 of 2019).

Article 4. (Amended, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 5. (Amended, SG No 103 of 2005, supplemented, repealed, SG No 17 of 2019).

## **Chapter Two**

### **COMMISSION FOR PERSONAL DATA PROTECTION**

Article 6. (1) (Amended, SG No 17 of 2019) The Commission for Personal Data Protection, hereinafter referred to as “the Commission”, shall be an independent supervisory authority which protects the individuals with regard to the processing of their personal data and the access to this data, as well as the supervision on the compliance with Regulation (EU) 2016/679 and with this Act.

(2) (New, SG No 94 of 2010) The Commission shall provide assistance with the implementation of the state policy in the personal data protection field.

(3) (Supplemented, SG No 91 of 2006, in force as from 1 January 2007, renumbered from Paragraph (2), SG No. 94 of 2010, amended, SG No 15 of 2013, in force as from 1 January 2014, amended, SG No 17 of 2019) The Commission shall be a state budget financed legal person with a main office in Sofia, and the Chairperson shall be a first-level budget spender.

Article 7. (1) The Commission shall consist of a Chairperson and four members.

(2) (Amended, SG No 91 of 2006, supplemented, SG No 17 of 2019) The members of the Commission and the Chairperson shall be elected by the National Assembly after a nomination by the Council of Ministers for a five years term and may be elected for one more term. The Chairperson and the members of the Commission shall continue to exercise their functions after the expiry of their

mandate until a new Chairperson and members are elected.

(3) The Chairperson and the members of the Commission shall carry out the activity under labour contracts.

(4) (New - SG 91/06, suppl. - SG 11/23, in force from 04.05.2023) The members of the Commission shall receive basic monthly remuneration equivalent to 2.5 average monthly wages received under labour and civil service contract in accordance with the information provided by the National Statistical Institute, increased by 20 percent. The basic monthly remuneration shall be recalculated every three months, taking into consideration the average monthly wage for the previous three months.

(5) (New, SG No 91 of 2006) The Chairperson of the Commission shall receive a monthly remuneration which is 30 per cent higher than the basic monthly remuneration referred to in Paragraph (4).

(6) (Amended, SG No 103 of 2005, renumbered from Paragraph (4), SG No 91 of 2006, amended, SG No 17 of 2019) The Commission shall submit an annual activity report to the National Assembly by 31 March.

Article 8. (1) Eligible to be members of the Commission are Bulgarian citizens who:

1. hold a university degree in information science or in law or hold a master's degree in information technology;
2. have not less than ten years working experience under labour contract;
3. (Supplemented, SG No 103 of 2005) have not been sentenced to prison for criminal offences, regardless of whether they have been rehabilitated.

(2) The following shall be ineligible for membership of the Commission  
Members of the Commission shall not be:

1. (Amended, SG No 103 of 2005) any persons who are sole traders, managing directors/insolvency practitioners or members of management bodies or supervisory bodies of entities, cooperatives or data controllers within the meaning of this Act;
2. any persons who hold another remunerable position, except where they engage in scientific research or teaching;
3. (New, SG No 42 of 2009) any persons who are spouses or *de facto* cohabitants, lineal descendants, collateral relatives up to the fourth degree of consanguinity or affines up to the second degree of affinity, of another member of the Commission.

(3) A qualified lawyer who meets the requirements under Paragraphs (1) and (2) shall be elected chairperson of the Commission.

(4) The term of office of the Chairperson or a member of the Commission shall be ended before the end of their mandate:

1. upon death or judicial disability;
2. by a resolution of the National Assembly, where:
  - (a) he or she has submitted a resignation;
  - (b) he or she has committed a serious infringement of this Act;
  - (c) he or she has committed a criminal offence, for which there is an imposed sentence;
  - (d) he or she is unable to fulfil their obligations for a period longer than six months;

(e) (New, SG No 42 of 2009, amended, SG No 97 of 2010, in force as from 10 December 2010, SG No 7 of 2018) there is a conflict of interest pursuant the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act.

(5) (Amended and supplemented, SG No 103 of 2005) In the cases referred to in Paragraph (4), the Council of Ministers shall make a proposal to the National Assembly for the election of a new member that shall serve the remainder of the original term of the member of the Commission concerned.

(6) The tenure of a chairperson or member of the Commission shall be equal to that of a civil servant under the Civil Servants Act.

(7) (New, SG No 103 of 2017, in force as from 1 January 2018) The circumstances referred to in Item 3 of Paragraph (1) shall be ascertained *ex officio* by the nominating authority.

Article 9. (1) (Amended, SG No 17 of 2019) In exercising its activity, the Commission shall be supported by an administration.

(2) (Amended, SG No 17 of 2019) The Commission regulates its activity, the activity of its administration, as well as the administrative proceedings with Rules of Procedure that are promulgated in the *State Gazette*.

(3) The Commission shall adopt decisions by a majority of the total number of its members.

(4) The meetings of the Commission shall be open to the public. The Commission may decide to hold closed meetings.

(5) (New - SG 11/23, in force from 04.05.2023) The meetings of the Commission, in which decisions are taken in implementation of the Act on the Protection of Persons, Reporting Information or Publicly Disclosing Information on Breaches, shall be closed.

Article 10. (1) (New, SG No 17 of 2019) The Commission shall fulfil the tasks pursuant to Article 57 of Regulation (EU) 2016/679.

(2) (Repealed, renumbered from Paragraph (1), amended, SG No 17 of 2019) In addition to the tasks referred to in Paragraph (1), the Commission shall:

1. analyse and exercise supervision and ensure compliance with Regulation (EU) 2016/679, with this Act and with the statutory instruments in the personal data protection field, except for the cases under Article 17;

2. issue secondary legislation acts in the personal data protection field;

3. ensure the implementation of the decisions of the European Commission in the personal data protection field and the implementation of the legally binding decisions of the European Data Protection Board under Article 65 of Regulation (EU) 2016/679;

4. participate in international cooperation with other personal data protection authorities and international organisations on personal data protection issues;

5. participate in the negotiations and the conclusion of bilateral or multilateral agreements on matters within its competence;

6. organise, coordinate and provide personal data protection training;

7. issue general and statutory administrative acts related to the its powers in cases foreseen in law.

(3) (Supplemented, SG No 103 of 2005, amended, SG No 91 of 2006) The Commission shall issue a bulletin where the Commission shall publish information on its activity and on the adopted decisions. The activity report pursuant to Article 7 (6) shall also be published in the bulletin.

(4) (New, SG No 103 of 2005, amended, SG No 91 of 2006, repealed, SG No 17 of 2019).

Article 10a. (New, SG No 17 of 2019) (1) The Commission shall exercise the powers pursuant to Article 58 of Regulation (EU) 2016/679.

(2) The Commission has also the following powers:

1. to refer any infringement of Regulation (EU) 2016/679 to the court;
2. to give instructions, issue guidelines, recommendations and best practices in connection with personal data protection.

Article 10b. (New, SG, 17/19, amend. - SG 11/23, in force from 04.05.2023)

(1) The Commission shall perform the functions of a central body for external whistleblowing in the sense of the Act on the Protection of Persons Reporting Information or Publicly Disclosing Information on Breaches.

(2) The Commission may be assigned other tasks and powers only by an Act.

Article 10c. (New, SG No 17 of 2019) (1) The Commission shall participate in the consistency mechanism pursuant Article 63 of Regulation (EU) 2016/679 and shall cooperate with the lead supervisory authority or the concerned supervisory authorities of the European Union Member States, including sharing information, providing or requesting mutual assistance or participating in joint operations in accordance with Regulation (EU) 2016/679.

(2) The forms of participation in the consistency mechanism, the provision and request for mutual assistance and the participation in joint operations, as well as the implementing procedures, shall be governed by the Rules of Procedure referred to in Article 9 (2).

Article 10d. (New, SG No 17 of 2019) When exercising the tasks and powers with regard to micro, small and medium-sized enterprises, acting as data controllers and processors, under Article 3 of the Small and Medium-Sized Enterprises Act, the Commission shall take consider the specific needs and the available resources of the enterprises.

Article 11. The Chairperson of the Commission shall:

1. organise and manage the activity of the Commission in compliance with the law and the decisions of the Commission and be responsible for the performance of the obligations;
2. represent the Commission in before third parties;
3. (Supplemented, SG No 103 of 2005, amended, SG No 81 of 2011) appoint and dismiss the civil servants, as well as conclude and terminate labour contracts of the administration employees under employment relationships;
4. (New, SG No 103 of 2005, amended, SG No 17 of 2019) issue penalty decrees under Article 87 (3).

Article 12. (Amended, SG No 91 of 2006) (1) (Amended, SG No 17 of 2019) The Chairperson and the members of the Commission or authorised staff by the Commission shall exercise control by means of prior consultation, inspections and joint operations in compliance with Regulation 2016/679 and with this Act.

(2) (Amended, SG No 17 of 2019) Except in the cases referred to in Article 36 (1) of Regulation (EU) 2016/679, prior consultation shall also take place where data are processed for the performance of a task carried out in public interest, including processing in relation to social protection and public health. In such a case, the Commission may authorise the processing before the period referred to

Article 36 (2) of Regulation (EU) 2016/679 expires.

(3) (Amended, SG No 17 of 2019) Prior consultation shall take place pursuant Article 36 (2) and (3) of Regulation (EU) 2016/679.

(4) (Amended, SG No 17 of 2019) Inspections shall be conducted on the initiative of the Commission, at the request of stakeholders, or after an alert has been submitted.

(5) The inspectors shall identify themselves by an official identity card and an order issued by the Chairperson of the Commission for the inspection concerned.

(6) When inspections are conducted, the persons referred to in Paragraph (1) may assign the preparation of expert examinations pursuant the Code of Civil Procedure.

(7) An inspection shall be concluded by a statement of findings.

(8) (Amended, SG No 17 of 2019) Where an administrative infringement is ascertained in the course of the inspection, administrative penalty proceedings shall be initiated.

(9) (New, SG No 7 of 2019) Without prejudice to the administrative fine, a coercive administrative measure under Chapter Nine may be imposed in the case of an administrative infringement.

(10) (Renumbered from Paragraph (9), SG No 17 of 2019) The conditions and procedure for the implementation of control shall be laid down instruction of the Commission.

(11) (New, SG No 17 of 2019) Joint operations with supervisory authorities of other Member States of the European Union, pursuant Article 62 of Regulation (EU) 2016/679, shall be conducted where appropriate for joint investigations and joint enforcement measures and shall involve, in addition to the persons referred to in Paragraph (1), also members or authorised staff of the supervisory authority of the Member State of the European Union concerned.

Article 12a. (New, SG No 17 of 2019) (1) When requested to do so, the data controller and processor shall provide assistance to the Commission in the fulfilment of its tasks and powers

(2) Where a duty of professional secrecy of the data controller or processor or another obligation of secrecy arising from a law may be infringed in exercising of the powers of the Commission pursuant points (e) and (f) of Article 58 (1) of Regulation (EU) 2016/679, the data controller or processor shall refuse access only to the information covered by the obligation of secrecy.

(3) Where the information contains data that is considered classified information, the procedure for access pursuant the Classified Information Protection Act shall apply.

Article 13. (Amended, SG No 103 of 2005) (1) The Chairperson, the members of the Commission and the administration shall be obliged not to disclose and not to take advantage of their own or another's benefit of the information considered a secret protected by law that has become known in the course of conducting its activity, until the period for protection of any such information has expired.

(2) Upon employment, the persons referred to in Paragraph (1) shall submit a declaration regarding the obligations under Paragraph (1).

(3) (New, SG No 17 of 2019) The Chairperson, the members of the Commission and the administration that are appointed by a labour contract shall be entitled to presentable clothing with a value of up to two minimum wages each year,

and the financial resources shall be allocated from the budget of the Commission. The individual amount of the financial resources shall be determined by the Chairperson of the Commission under terms and a procedures established by the Rules of Procedure pursuant referred to in Article 9 (2).

Article 14. (Amended, SG No 103 of 2005, amended, SG No 17 of 2019) (1) The Commission shall conduct accreditation of certification bodies in pursuant Regulation (EU) 2016/679 on the basis of the requirements laid down by the Commission or by the European Data Protection Board.

(2) The accreditation shall be issued in accordance with Article 43 (2) of Regulation (EU) 2016/679 for a period of five years and may be renewed.

(3) The Commission shall withdraw the accreditation of a certification body when the conditions for accreditation laid down are not met or where actions taken by the certification body infringe this Act or Regulation (EU) 2016/679.

(4) The decisions of the Commission regarding the withdrawal of an accreditation under Paragraph (3) can be appealed pursuant the Administrative Procedure Code.

(5) The conditions, including the requirements referred to in Paragraph (1), and the procedure for accreditation and its withdrawal shall be laid down in an ordinance adopted by the Commission. The ordinance shall be promulgated in the *State Gazette*.

(6) The certification criteria, mechanisms and procedures, seals and marks shall be laid down in an ordinance adopted by the Commission. The ordinance shall be promulgated in the *State Gazette*.

Article 14a. (New, SG No 17 of 2019) (1) The Commission shall approve codes of conduct by sector and field of action pursuant to Article 40 of Regulation (EU) 2016/679. The conditions, procedure and criteria for the approval of the codes of conduct shall be established by the Rules of Procedure referred to in Article 9 (2).

(2) The Commission shall conduct the accreditation of bodies for monitoring the codes of conduct approved pursuant to Paragraph (1) in accordance with Article 41 of Regulation (EU) 2016/679.

(3) The requirements for accreditation under Paragraph (2) and the procedure for accreditation and withdrawal of the accreditation shall be established by an ordinance adopted by the Commission. The ordinance shall be promulgated in the *State Gazette*.

(4) The Commission shall withdraw the accreditation of a body monitoring approved codes of conduct where the conditions for accreditation are not met or where actions taken by the body infringe this Act or Regulation (EU) 2016/679.

(5) The decisions of the Commission with regard to the withdrawal of an accreditation under Paragraph (4) shall be appealable under the procedure of the Administrative Procedure Code.

Article 15. (Repealed, SG No 103 of 2005, new, SG No 17 of 2019) (1) The Commission shall maintain the following public registers:

1. a register of data controllers and processors which have designated data protection officers;
2. a register of certification bodies accredited pursuant Article 14;
3. a register of codes of conduct pursuant Article 40 of Regulation (EU) 2016/679.

(2) The Commission shall maintain the following registers which shall not be public:

1. a register of the infringements of Regulation (EU) 2016/679 and this Act, as well as of the measures taken in accordance with the exercise of the powers referred to in Article 58 (2) of Regulation (EU) 2016/679;

2. a register of the notifications of personal data breaches under Article 33 of Regulation (EU) 2016/679 and under Article 67.

(3) The procedure for the establishment and maintenance of the registers referred to in Paragraphs (1) and (2) and the access shall be pursuant the Electronic Governance Act, and the content of the registers shall be laid down by the Rules of Procedure referred to in Article 9 (2).

Article 16. (Amended, SG No 103 of 2005, repealed, SG No 91 of 2006, new, SG No 17 of 2019) (1) The conditions and procedure for the carrying out of training pursuant Item 6 of Article 10 (2) shall be established by the Rules of Procedure referred to in Article 9 (2).

(2) The Commission shall issue a certificate to the persons who have participated in a training under Paragraph (1) after an examination has been successfully passed. The certificate shall be valid for three years. After the period of time referred to in sentence two has expired, a certificate shall be renewed after an examination has been successfully passed under terms and a procedure established by the Rules of Procedure referred to in Article 9 (2).

(3) The availability of a certificate under Paragraph (2) may not be mandatory for the appointment or acting in the capacity of a data protection officer.

(4) Fees shall be charged for the training under Paragraph (1), except in the cases of training organised and delivered on the initiative of the Commission. The fees shall be set by a rate schedule approved by the Council of Ministers on a proposal by the Commission.

### **Chapter Three**

#### **INSPECTORATE TO THE SUPREME JUDICIAL COUNCIL (HEADING AMENDED, SG No 103 OF 2005, AMENDED, SG No 17 OF 2019)**

Article 17. (Amended, SG No 103 of 2005, amended, SG No 91 of 2006, amended, SG No 17 of 2019) (1) The Inspectorate of the Supreme Judicial Council, hereinafter referred as “the Inspectorate”, shall exercise supervision and shall ensure compliance with Regulation (EU) 2016/679, with this Act and with the statutory instruments in the field of personal data protection upon the processing of personal data by:

1. the court when acting in the judicial capacity; and

2. the prosecution and the investigating authorities when acting in the judicial capacity for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(2) The procedure for implementing the activity referred to in Paragraph (1), including the conducting of inspections and for the proceedings before the Inspectorate, shall be established by the rules referred to in Article 55 (8) of the Judicial System Act.

(3) Article 12a shall furthermore apply in the course of the supervision under Paragraph (1).



Article 17a. (New, SG No 91 of 2006, amended, SG No 17 of 2019) (1) In the course of exercising the supervision of the processing of personal data by the court when acting in the judicial capacity, except for the processing of personal data for the purposes referred to in Article 42 (1), the Inspectorate shall:

1. fulfil the tasks pursuant points (a) to (i), (l), (u) and (v) of Article 57 (1) and Article 57 (2) and (3) of Regulation (EU) 2016/679;

2. exercise the powers pursuant points (a), (b), (d), (e), (f) of Article 58 (1), points (a) to (g), (i) and (j) of Article 58 (2) and points (a), (b) and (c) of Article 58 (3) of Regulation (EU) 2016/679;

3. apply, *mutatis mutandis*, the list pursuant Article 35 (4) of Regulation (EU) 2016/679 in connection with the requirement for a data protection impact assessment;

4. bring any infringement of Regulation (EU) 2016/679 to the attention of the court.

(2) In addition to the tasks and powers referred to in Paragraph (1), the Inspectorate shall:

1. participate in international cooperation with other personal data protection authorities and international organisations on issues in the field of personal data protection;

2. give instructions, issue guidelines, recommendations and best practices in connection with personal data protection.

(3) In the course of exercising the supervision with regard to the processing of personal data for the purposes referred to in Article 42 (1) by the court, the prosecution and the investigating authorities when acting in the judicial capacity, the Inspectorate shall fulfil the tasks and shall exercise the powers under Chapter Eight.

Article 17b. (New, SG No 91 of 2006, amended, SG No 17 of 2019) (1) The Inspectorate shall carry out prior consultation:

1. in the cases pursuant Article 36 (1) of Regulation (EU) 2016/679;

2. for the processing of personal data for the performance of a task carried out in the public interest; in this case, the Inspectorate may authorise the processing before the period referred to in Article 36 (2) of Regulation (EU) 2016/679 has expired.

(2) Prior consultation shall take place in pursuant Article 36 (2) and (3) of Regulation (EU) 2016/679.

Article 18. (Amended, SG No 103 of 2005, amended, SG No 17 of 2019) (1) In the course of exercising the supervision under Article 17 (1), the Inspectorate shall conduct inspections envisaged in its annual programme or responding to alerts. A publication in the mass media shall also be eligible as an alert.

(2) The inspection shall be conducted by the Inspector General or by an inspector, who shall be assisted by experts, on the basis of an order of the Inspector General.

Article 19. (Supplemented, SG No 93 of 2004, amended, SG No 103 of 2005, amended, SG No 17 of 2019) (1) The inspection shall be concluded by a written statement setting out the results and findings and, where necessary, shall make recommendations.

(2) Where an infringement of Regulation (EU) 2016/679 and of this Act is ascertained during the inspection, depending on the nature and extent of the

infringement, the measures referred to in points (a) to (g) and (j) of Article 58 (2) of Regulation (EU) 2016/679 or in Items 3, 4 and 5 of Article 80 (1) shall be applied or administrative fines shall be imposed in accordance with Article 83 of Regulation (EU) 2016/679 and under Chapter Nine.

(3) The measures referred to in points (a) to (g) and (j) of Article 58 (2) of Regulation (EU) 2016/679 or in Items 3, 4 and 5 of Article 80 (1) shall be applied with a decision of the Inspectorate on a proposal by the inspector who conducted the inspection.

Article 20. (Amended, SG No 103 of 2005, amended, SG No 17 of 2019) The chairperson and the members of the Commission and the administration shall be obliged not to disclose and not to take advantage of their own or another's benefit of the information constituting a secret protected by law that has become known in the course of conducting its activity, until the period for protection of any such information has expired.

Article 21. (Amended, SG No 103 of 2005, amended, SG No 17 of 2019) (1) The Inspectorate shall keep the following registers, which shall not be public:

1. a register of infringements of Regulation (EU) 2016/679 and of this Act, as well as of the measures taken in accordance with the exercise of the powers referred to in points (a) to (g), (i) and (j) of Article 58 (2) of Regulation (EU) 2016/679;

2. a register of notifications of personal data breaches under Article 33 of Regulation (EU) 2016/679 and under Article 67.

(2) The procedure for the establishment and maintenance of the registers referred to in Paragraph (1) and the access thereto shall be established in accordance with the Electronic Governance Act, and the content of the said registers shall be determined by the rules referred to in Article 55 (8) of the Judicial System Act.

Article 22. (Amended, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 22a. (New, SG No 91 of 2006, repealed, SG No 17 of 2019).

#### **Chapter Four**

#### **DATA PROTECTION OFFICER (REPEALED, SG No 17 OF 2019)**

Article 23. (Amended, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 23a. (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

Article 23b. (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

Article 24. (Repealed, SG No 17 of 2019).

Article 25. (Repealed, SG No 17 of 2019).

#### **Chapter Four A**

#### **COMMON RULES WITH REGARD TO PROCESSING OF PERSONAL DATA. SPECIFIC DATA PROCESSING CASES (NEW, SG No 17 OF 2019)**

Article 25a. (New, SG No 17 of 2019) Where any personal data has been provided by the data subject to a data controller or processor without legal basis pursuant Article 6 (1) of Regulation (EU) 2016/679 or contrary to the principles under Article 5 of the same Regulation, the data controller or processor shall return such data within a period of one month after having become aware of it or, if this is impossible or would involve disproportionate efforts, shall erase or destroy the data. The erasure and destruction shall be documented.

Article 25b. (New, SG No 17 of 2019) The data controller and processor shall notify the Commission of the full name, the personal identification number or the foreigner personal number or another similar identifier, and of the contact details of the data protection officer, as well as of any ensuing changes. The form and content of the notification and the procedure for the submission of the said notification shall be determined by the Rules of Procedure pursuant Article 9 (2).

Article 25c. (New, SG No 17 of 2019) The processing of the data of a data subject who is under the age of 14 years based on consent within the meaning of point 11 of Article 4 of Regulation (EU) 2016/679, including the cases where information society services are offered directly within the meaning of Article 1 (3) of the Electronic Commerce Act, shall be lawful only if that consent of a parent with parental rights or by a legal guardian is given.

Article 25d. (New, SG No 17 of 2019) A data controller or processor may copy an identity document, a motor vehicle driving licence or a residence document only if this is laid down in a law.

Article 25e. (New, SG No 17 of 2019) (1) The data controller or processor shall adopt and apply rules for large scale personal data processing or for a large scale systematic monitoring of publicly accessible areas, including video surveillance, if the controller or processor implements appropriate technical and organisational measures for safeguarding the rights and freedoms of data subjects. The rules on large scale systematic monitoring of publicly accessible areas shall state the legal grounds for setting up a monitoring system, its scope and means, storage period of the information records and their erasure, the individuals' right of access, the provision of information to the public about the monitoring, as well as restrictions with regard to the access of third parties.

(2) The Commission shall issue guidelines to data controllers and processors for the performance of the obligation under Paragraph (1) and shall publish them on its Internet site.

Article 25f. (New, SG No 17 of 2019) (1) A data controller or processor may process personal data of deceased persons only if there is a legal basis for this. In such cases, the data controller or processor shall take the appropriate measures so that the rights and freedoms of others or a public interest would not be adversely affected.

(2) (Suppl. - SG 11/23, in force from 04.05.2023) The Administrator shall provide, upon request, access to the personal data of a deceased person, including a copy thereof, to his heirs or other persons with legal interest, within the terms under Art. 12, paragraphs 3 and 4, and under the terms of paragraphs 5 and 6 of Regulation (EU) 2016/679, unless otherwise provided by law.

Article 25g. (New, SG No 17 of 2019) (1) Free public access to any information containing a personal identification number or a foreigner personal number shall not be provided unless otherwise foreseen in law.

(2) Controllers providing services by electronic means shall take appropriate technical and organisational measures to ensure that the personal identification number or the foreigner personal number is not the only means of identifying the user when remote access to the service is provided.

(3) In order to provide administrative services by electronic means under the conditions of the Electronic Governance Act, the controller shall make it possible for the data subject to identify himself or herself following a procedure envisaged in law.

Article 25h. (New, SG No 17 of 2019) (1) The processing of personal data for journalistic purposes and for the purposes of academic, artistic or literary expression shall be lawful when carried out on the ground of freedom of expression and the right to information while simultaneously respecting privacy.

(2) (Declared unconstitutional with Decision of the Constitutional Court No 8 of 2019 – SG 93 of 2019) **In case of disclosure by transmission, dissemination or otherwise making available the personal data collected for the purposes under paragraph (1), the balance between the freedom of expression and the right to information and the right of personal data protection shall be evaluated on the basis of the following criteria, if relevant:**

1. nature of the personal data;
2. the impact that the disclosure of the personal data or the publishing of the data would have on the data subject's privacy and reputation;
3. the circumstances under which the personal data became known to the controller;
4. the character and nature of the statement under which the rights referred to in paragraph (1) are exercised;
5. the significance of the disclosure of personal data or the publishing of the data for the clarification of a matter of public interest;
6. taking into consideration whether the data subject occupies position under Article 6 of the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act or is a person who, because of his activity and public status enjoys lesser protection of his privacy, or whose actions impact the society;
7. taking into consideration whether the data subject has contributed with his actions for the disclosure of his personal data and/or of information about his private and family life;
8. the purpose, content, form and consequence of the statement when the rights pursuant paragraph (1) are exercised;
9. the compliance of the statement for exercising the rights paragraph (1) with the fundamental rights of citizens;
10. other circumstances relevant to the case.

(3) Where personal data are processed for the purposes of paragraph (1):

1. Articles 6, 9, 10, 30, 34 and Chapter V of Regulation (EU) 2016/679, as well as Article 25c, shall not apply;

2. the data controller or processor may deny the data subjects, fully or partially the exercise of the rights pursuant Articles 12 to 21 of Regulation (EU) 2016/679.

(4) The exercise of the powers of the Commission pursuant to Article 58 (1) of

Regulation (EU) 2016/679 shall not affect the secrecy of information sources.

(5) Where personal data are processed for the purposes of creating a photographic or audio-visual work by means of capturing the image of a person in the course of the public activity or in a public place, Article 6, Articles 12 to 21, and Articles 30 to 34 of Regulation (EU) 2016/679 shall not apply.

Article 25i. (New, SG No 17 of 2019) (1) Any employer or appointing authority, in the capacity of data controller, shall adopt rules and procedures for:

1. use of an infringements reporting system;
2. restrictions on the use of internal company resources;
3. implementation of control system for access, working time and discipline.

(2) The rules and procedures referred to in Paragraph (1) shall contain information relating to the scope, obligations and methods for its practical application. These shall take into consideration the activity of the employer or appointing authority and the related nature of work and may not restrict the rights of data subjects pursuant Regulation (EU) 2016/679 and pursuant this Act.

(3) Employees and workers shall be informed of the rules and procedures referred to in Paragraph (1).

Article 25j. (New, SG No 17 of 2019) (1) Any appointing authority, in the capacity of data controller, shall determine a storage period for the personal data of candidates in staff selection procedures which may not be longer than six months, unless the applicant has given consent for a longer period of storage. When the period of time expires, the employer or appointing authority shall erase or destroy the documents containing personal data unless otherwise provided for by a special law.

(2) Where in a staff selection procedure under Paragraph (1) the employer or appointing authority has required the submission of originals or copies certified by a notary, ascertaining the physical and mental fitness of the applicant, the required qualification degree and experience for the position held, the employer or authority shall return the documents to the data subject who has not been approved for appointment within six months of the completion of the selection procedure unless otherwise provided for by a special law.

Article 25k. (New, SG No 17 of 2019) The processing of personal data for the purposes of the National Archive Funds of the Republic of Bulgaria shall be processing in the public interest. Articles 15, 16, 18, 19, 20 and 21 of Regulation (EU) 2016/679 shall not apply in such cases.

Article 25l. (New, SG No 17 of 2019) Where personal data is processed for statistical purposes, Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 shall not apply.

Article 25m. (New, SG No 17 of 2019) Personal data originally collected for a different purpose may be processed for the purposes of the National Archive Funds, for scientific, for historical research or for statistical purposes. In such cases, the controller shall apply appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject in accordance with Article 89 (1) of Regulation (EU) 2016/679.

Article 25n. (New, SG No 17 of 2019) The processing of personal data for humanitarian purposes by public bodies or humanitarian organisations, as well as the processing in cases of disaster within the meaning of the Disaster Protection Act, shall be lawful. Articles 12 to 21 and Article 34 of Regulation (EU) 2016/679 shall not apply in this case.

**Chapter Five**  
**RIGHTS OF NATURAL PERSONS (HEADING AMENDED, SG No 103 OF**  
**2005, REPEALED, SG No 17 OF 2019)**

Article 26. (Repealed, SG No 17 of 2019).

Article 27. (Amended, SG No 103 of 2005, repealed, SG No 91 of 2006).

Article 28. (Amended, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 28a. (New, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 29. (Repealed, SG No 17 of 2019).

Article 30. (Amended, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 31. (Repealed, SG No 17 of 2019).

Article 32. (Amended, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 33. (Repealed, SG No 17 of 2019).

Article 34. (Repealed, SG No 17 of 2019).

Article 34a. (New, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 34b. (New, SG No 103 of 2005, repealed, SG No 17 of 2019).

**Chapter Six**  
**PROVISION OF PERSONAL DATA TO THIRD PARTIES (REPEALED, SG**  
**No 17 OF 2019)**

Article 35. (Amended, SG No 103 of 2005, repealed, SG No 91 of 2006).

Article 36. (Amended, SG No 103 of 2005, in force as from 1 January 2007, repealed, SG No 17 of 2019).

Article 36a. (New, SG No 103 of 2005, in force as from 1 January 2007, repealed, SG No 17 of 2019).

Article 36b. (New, SG No 103 of 2005, in force as from 1 January 2007, repealed, SG No 17 of 2019).

Article 36c. (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

Article 36d. (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

Article 36e. (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

Article 36f. (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

Article 36g. (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

Article 36h. (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

Article 36i. (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

Article 37. (Repealed, SG No 103 of 2005).

## **Chapter Seven**

### **EXERCISE OF DATA SUBJECT RIGHTS. REMEDIES (HEADING AMENDED, SG No 17 OF 2019)**

Article 37a. (New, SG No 17 of 2019) (1) The data controller or processor may deny the data subjects the exercise, wholly or partially, of the rights pursuant Articles 12 to 21 of Regulation (EU) 2016/679 and may not perform the obligation pursuant Article 34 of Regulation (EU) 2016/679 where the exercise of the rights or the performance of the obligation would result in a risk to:

1. national security;
2. defence;
3. public order and security;
4. the prevention, investigation, detection or prosecution of criminal offences or the enforcement of criminal penalties, including the safeguarding and the prevention of threats to public security;
5. other important objectives of general public interest, in particular an important economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;
6. the safeguarding of judicial independence and judicial proceedings;
7. the prevention, investigation, detection and prosecution of breaches of codes of ethics for specifically regulated professions;
8. the protection of the data subject or the rights and freedoms of others;
9. the enforcement of civil law claims.

(2) The conditions and procedure for the application of Paragraph (1) shall be established by law and in accordance with Article 23 (2) of Regulation (EU) 2016/679.

Article 37b. (New, SG No 17 of 2019) (1) The data subject shall exercise the rights pursuant Articles 15 to 22 of Regulation (EU) 2016/679 by submitting a written

application to the data controller or by another method determined by the controller.

(2) Alternatively, an application may be submitted by electronic means under the conditions of the Electronic Document and Electronic Trust Services Act, the Electronic Signature Act, the Electronic Governance Act and the Electronic Commerce Act.

(3) Alternatively, an application may be submitted by accessing the user interface of the data processing information system after the person has identified himself or herself by the means of identification, relevant to the information system.

Article 37c. (New, SG No 17 of 2019) The application pursuant to Article 37b shall contain:

1. name, address, personal identification number or foreigner personal number or another similar identifier, of other data determined by the controller identifying the natural person, in relation to his/her activity;
2. description of the request;
3. preferred form in which information is to be received for the exercise of the rights under Articles 15 to 22 of Regulation (EU) 2016/679;
4. signature, date of submission of the application and address for correspondence.

(2) Where an application is submitted by an authorised person, the power of attorney shall be attached to the application.

Article 38. (1) (Amended, SG No 103 of 2005, amended, SG No 91 of 2006, amended, SG No 17 of 2019) In cases of infringement of his/her rights pursuant to Regulation (EU) 2016/679 and this Act, the data subject shall have the right to bring the infringement before Commission within six months after having become aware of the infringement but no later than two years after.

(2) (New, SG No 17 of 2019) The Commission shall inform the complainant of the progress of the complaint or of the result within three months after the infringement has been brought to the attention of the Commission.

(3) (Amended, SG No 103 of 2005, renumbered from Paragraph (2), amended, SG No 17 of 2019) The Commission shall issue a decision and may apply the measures referred to in points (a) to (h) and (j) of Article 58 (2) of Regulation (EU) 2016/679 or in Items 3, 4 and 5 of Article 80 (1) and, in addition to or instead of them, the Commission may impose an administrative fine in accordance with Article 83 of Regulation (EU) 2016/679 and under Chapter Nine.

(4) (New, SG No 17 of 2019) Where the complaint is obviously unfounded or excessive, the Commission may adopt a decision to dismiss the complaint.

(5) (Renumbered from Paragraph (4), amended, SG No 17 of 2019) The Commission shall send a copy of the decision to the data subject as well.

(6) (New, SG No 91 of 2006, renumbered from Paragraph (5), amended, SG No 17 of 2019) In the cases referred to in Paragraph (1), where personal data is processed for the purposes referred to in Article 42 (1), the decision of the Commission shall contain only a finding about the lawfulness of the processing.

(7) (New - SG 11/23, in force from 04.05.2023) Complaint under Para. 1 may be withdrawn until the expiry of the period for appealing the decision of the Commission under Para. 3 and 4.

(8) Amend. - SG, 103/05, previous Para. 5 - SG, 91/06, amend. - SG, 39/11, previous Para. 6, amend. - SG, 17/19, previous Para. 7 - SG 11/23, in force from 04.05.2023) The decision of the Commission pursuant Paragraphs (3) and (4) is a



subject of appeal pursuant to the Administrative Procedure Code within 14 days of receipt.

Article 38a. (New, SG No 17 of 2019) (1) The complaint to the Commission may be submitted by a letter, fax or by electronic means under the procedure of the Electronic Document and Electronic Trust Services Act.

(2) No action shall be taken on anonymous complaints and on complaints which are not signed by the complainant or by a legal or authorised representative.

Article 38b. (New, SG No 17 of 2019) (1) By any infringement of the rights under Regulation (EU) 2016/679 and under this Act with the processing of personal data by the court when acting in the judicial capacity and by the prosecution and the investigating authorities when acting in the judicial capacity for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, the data subject shall have the right to submit a complaint to the Inspectorate within six months after becoming aware of the infringement but not later than two years after the infringement.

(2) In the cases referred to in Paragraph (1), Article 38a shall apply, *mutatis mutandis*.

Article 38c. (New, SG No 17 of 2019) (1) The complaint pursuant Article 38b (1) shall be examined by an inspector designated by the Inspector General on the basis of the random selection principle.

(2) Data relevant to the alleged infringement shall be collected when handling the complaint, including information from the data controller or processor.

(3) The complainant shall be informed of the progress of the complaint or of its result within three months after the infringement has been brought to the attention of the Inspectorate.

(4) Where the complaint is unfounded, the inspector shall give his or her decision which could be appealed pursuant to the Administrative Procedure Code within 14 days of reception of the decision.

(5) Where the complaint is founded, the Inspectorate shall issue a decision on a proposal by the inspector. The decision could be appealed pursuant to the Administrative Procedure Code within 14 days of reception of the decision.

(6) Where the complaint is unfounded or excessive, the inspector may dismiss it.

Article 38d. (New, SG No 17 of 2019) (1) Where an infringement of Regulation (EU) 2016/679 is ascertained in proceedings under Article 38c, depending on the nature and extent of the infringement, the measures referred to in points (a) to (g) and (j) of Article 58 (2) of Regulation (EU) 2016/679 or in Items 3, 4 and 5 of Article 80 (1) shall be applied or administrative fines shall be imposed in accordance with Article 83 of Regulation (EU) 2016/679 and under Chapter Nine.

(2) The measures referred to in points (a) to (g) and (j) of Article 58 (2) of Regulation (EU) 2016/679 and in Items 3, 4 and 5 of Article 80 (1) shall be applied by a decision of the Inspectorate on a proposal by the inspector who examined the complaint under Article 38b (1).

Article 39. (1) (Amended, SG No 103 of 2005, amended, SG No 30 of 2006, in force as from 1 March 2007, amended, SG No 91 of 2006, amended, SG No 17 of 2019) Upon any infringement of the rights pursuant to Regulation (EU) 2016/679 and pursuant to this Act, the data subject may appeal against any actions or acts of the data controller and processor before the court pursuant to the Administrative Procedure Code.

(2) (Amended, SG No 103 of 2005, amended and supplemented, SG No 17 of 2019) In the proceedings under Paragraph (1), the data subject may claim compensation for the damage suffered as a result of an unlawful processing of personal data from the data controller or processor.

(3) (New, SG No 81 of 2011, repealed, SG No 17 of 2019).

(4) (New, SG No 103 of 2005, renumbered from Paragraph (3), SG No 81 of 2011, amended, SG No 17 of 2019) The data subject may not bring a violation to the attention of the court if proceedings on the same infringement are pending before the Commission or a decision of the Commission regarding the same infringement has been appealed and there is no enforceable judgment of the court. At the request of the data subject, the Commission shall certify the lack of proceedings pending before it on the same dispute.

(5) (Renumbered from Paragraph (4), amended, SG No 103 of 2005, amended, SG No 30 of 2006, in force as from 12 July 2006, repealed, SG No 91 of 2006, new, SG No 17 of 2019) Paragraph (4) shall apply on any proceedings pending before the Inspectorate.

Article 40. (Repealed, SG No 103 of 2005, new, SG No 17 of 2019) Where the decision referred to in Article 38 (3) has been adopted to implement a binding decision of the European Data Protection Board, Articles 263 and 267 of the Treaty on the Functioning of the European Union shall apply accordingly.

Article 41. (Repealed, SG No 103 of 2005).

## **Chapter Eight**

### **RULES ON PROTECTION OF NATURAL PERSONS WITH REGARD TO PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR PURPOSES OF PREVENTION, INVESTIGATION, DETECTION OR PROSECUTION OF CRIMINAL OFFENCES OR EXECUTION OF CRIMINAL PENALTIES, INCLUDING SAFEGUARDING AGAINST AND PREVENTION OF THREATS TO PUBLIC ORDER AND SECURITY (TITLE, AMEND. – SG, 17/19)**

#### **Section I**

##### **General Provisions (New, SG No 17 of 2019)**

Article 42. (Amended, SG No 103 of 2005, amended, SG No 17 of 2019) (1) The rules of this Chapter shall apply upon the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public order and security.

(2) Personal data collected for the purposes referred to in Paragraph (1) shall not be processed for any other purposes unless otherwise provided for by Union law

or by the legislation of the Republic of Bulgaria.

(3) Where the competent authorities under Paragraph (1) process personal data for any purposes other than those under Paragraph (1), as well as in the cases referred to in Paragraph (2), Regulation (EU) 2016/679 and the respective provisions of this Act which introduce measures for the application of the said Regulation shall apply.

(4) Competent authorities under Paragraph (1) shall be the public authorities vested with powers to prevent, investigate, detect or prosecute criminal offences or to execute criminal penalties, including to safeguard against and prevent threats to public security.

(5) Unless otherwise provided for by a law, controller within the meaning of this Chapter with regard to the processing of personal data for the purposes under Paragraph (1) shall be a competent authority referred to in Paragraph (4) or the relevant administrative structure the said authority is a part, which independently or jointly with other authorities determine the purposes and the means of processing personal data.

Article 42a. (New, SG No 103 of 2005, repealed, SG No 17 of 2019).

Article 43. (Amended, SG No 103 of 2005, amended, SG No 17 of 2019) The rules of this Chapter shall apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of any such system.

Article 44. (New, SG No 17 of 2019) The exchange of personal data between the competent authorities of the Member States of the European Union, where such exchange is required by Union law or the legislation of the Republic of Bulgaria, shall neither be restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 45. (New, SG No 17 of 2019) (1) Upon the processing of personal data for the purposes referred to in Article 42 (1), the personal data must be:

1. processed lawfully and fairly;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which the data are processed;
4. accurate and, where necessary, kept up to date; every requisite step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the said data are processed;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(2) Processing of personal data by a controller which originally collected the said data or by another controller for any of the purposes referred to in Article 42 (1) other than the purpose for which the said data have been originally collected shall be allowed provided that:

1. the controller is empowered to process personal data for any such purpose

in accordance with Union law or the legislation of the Republic of Bulgaria, and

2. the processing is necessary and proportionate to that different purpose in accordance with Union law or with the legislation of the Republic of Bulgaria.

(3) The processing by a controller under Paragraph (2) may include archiving in the public interest, scientific, statistical or historical use of the data for the purposes referred to in Article 42 (1) while applying appropriate safeguards for the rights and freedoms of data subjects.

(4) The controller shall be responsible for, and be able to demonstrate compliance with, Paragraphs (1), (2) and (3).

Article 46. (New, SG No 17 of 2019) (1) Where the time limits for the erasure of personal data or for a periodic review of the need for the storage are not statutorily established, the said time limits shall be established by the controller.

(2) The carrying out of a periodic review under Paragraph (1) shall be documented, and the decision to extend the storage of the data shall be reasoned.

Article 47. (New, SG No 17 of 2019) The controller, where applicable and as far as possible, shall make a clear distinction between personal data of different categories of data subjects, such as:

1. persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

2. persons convicted of a criminal offence;

3. victims of a criminal offence, or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

4. other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts.

Article 48. (New, SG No 17 of 2019) (1) The competent authority shall, as far as possible, distinguish personal data based on facts from personal data based on personal assessments.

(2) The competent authority shall take the requisite steps that personal data which are inaccurate, incomplete or no longer up to date are not transmitted. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.

(3) Where the transmitted personal data are incorrect or have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the transmitting competent authority and the recipient shall rectify, erase or restrict the processing of the personal data.

Article 49. (New, SG No 17 of 2019) The processing of personal data shall be lawful where necessary for the exercise of powers by a competent authority for the purposes referred to in Article 42 (1) and where provided for in Union law or in a statutory instrument which defines the purposes of the processing and the categories of personal data which are processed.

Article 50. (New, SG No 17 of 2019) (1) Where Union law or the legislation of the Republic of Bulgaria applicable to the transmitting competent authority provides specific conditions for processing of personal data, the authority shall inform the recipient of such personal data of those conditions and the obligation of the said recipient to comply with the said conditions.

(2) Personal data shall be transmitted to recipients in other Member States of the European Union, or to agencies, offices and bodies of the European Union established pursuant to Chapters 4 and 5 of Title V of the Treaty on the Functioning of the European Union under the same conditions which are applicable to similar transmissions within the Republic of Bulgaria.

Article 51. (New, SG No 17 of 2019) (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed where this is strictly necessary, there are appropriate safeguards for the rights and freedoms of the data subject, and is provided for in Union law or in the legislation of the Republic of Bulgaria.

(2) Where processing under Paragraph (1) is not provided for in Union law or in the legislation of the Republic of Bulgaria, the data referred to in Paragraph (1) may be processed where this is strictly necessary, there are appropriate safeguards for the rights and freedoms of the data subject, and:

1. the processing is necessary to protect the vital interests of the data subject or of another natural person, or

2. if the processing relates to data which are manifestly made public by the data subject.

(3) Suitable measures and safeguards for non-discrimination against natural persons shall be put in place where data are processed under Paragraph (1).

Article 52. (New, SG No 17 of 2019) (1) Any decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, shall be prohibited unless this is provided for in Union law or in the legislation of the Republic of Bulgaria and appropriate safeguards are provided for the rights and freedoms of the data subject, at least the right to obtain human intervention when the controller makes the decision concerned.

(2) Decisions referred to in Paragraph (1) may not be based on the categories of personal data referred to in Article 51 (1), unless suitable measures to safeguard the rights and freedoms and legitimate interests of the data subject are in place.

(3) In the cases under Paragraphs (1) and (2), the controller shall carry out an impact assessment under Article 64.

(4) Profiling that results in discrimination against natural persons on the basis of the categories of personal data referred to in Article 51 (1) shall be prohibited.

(5) The data subject shall have the right to obtain information on the processing referred to in Paragraph (1), to express his or her point of view, and to contest the decision.

## **Section II**

### **Data Subject Rights (New, SG No 17 of 2019)**

Article 53. (New, SG No 17 of 2019) (1) The controller shall take the requisite steps to provide any information referred to in Article 54 and make any communication with regard to Article 52 (5) and Articles 55 to 58 and 68 relating to processing of personal data to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The controller shall provide the information in the same form as the request. Where this is impossible or would involve disproportionate efforts, the information shall be provided by other appropriate means, including by electronic means.

(2) The controller shall facilitate the exercise of data subject rights under Article 52 (5) and Articles 55 to 58.

(3) The controller shall reply to the request of the data subject or shall inform the said subject in writing of the action taken on the request within two months of receipt of the request. That period may be extended by one further month where necessary, taking into account the complexity and number of the requests.

(4) Information under Article 54 and any communications or any actions taken under Article 52 (5), Articles 55 to 58 and 68 shall be provided free of charge. Where requests from a particular data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may:

1. charge a fee in an amount which takes into account the administrative costs of providing information or communication with the data subject or taking the action requested, or

2. refuse to act on the request.

(5) The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

(6) Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 55 or 56, the controller may request the provision of additional information necessary to confirm the identity of the data subject. The period referred to in Paragraph (3) shall begin to run from the receipt of that additional information.

Article 54. (New, SG No 17 of 2019) (1) The controller shall make available to the data subject at least the following information:

1. the identity and the contact details of the controller;
2. the contact details of the data protection officer, where applicable;
3. the purposes for which the personal data are processed;
4. the right to lodge a complaint with the Commission or, respectively, with the Inspectorate and the contact details;

5. the right to request from the controller access to and rectification, completion or erasure of personal data and restriction of processing of the personal data concerning the data subject;

6. the possibility, in the event of refusal under Paragraph (3), under Article 55 (3) and (4) and Article 56 (6) and (7), to exercise the rights through the Commission or, respectively, through the Inspectorate.

(2) In addition to the information referred to in Paragraph (1), at the request of the data subject or on its own initiative the controller shall give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:

1. the legal basis for the processing;
2. the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;
3. where applicable, the recipients or the categories of recipients of the personal data, including in third countries or international organisations;
4. where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

(3) The controller may delay or refuse, in whole or in part, the provision of the information referred to in Paragraph (2), where this is necessary in order to:

1. avoid obstructing official or legal checks, investigations or procedures;
2. avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
3. protect public order and security;
4. protect national security;
5. protect the rights and freedoms of others.

(4) When any circumstance referred to in Paragraph (3) ceases to apply, the controller shall provide without delay the requested information within the period referred to in Article 53 (3).

(5) In making a decision under Paragraph (3), the controller shall take into account the fundamental rights and legitimate interests of the natural person concerned.

Article 55. (New, SG No 17 of 2019) (1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the said data and information on:

1. the circumstances referred to in Items 3 to 5 of Article 54 (1) and Items 1 to 3 of Article 54 (2);
2. the categories of personal data concerned;
3. the personal data undergoing processing and any available information as to the origin, unless the said information constitutes a secret protected by law.

(2) The controller shall provide the information referred to in Paragraph (1) within the period referred to in Article 53 (3).

(3) The right of access to the data and the information referred to in Paragraph (1) may be wholly or partly restricted taking into account the fundamental rights and legitimate interests of the natural person concerned in the cases referred to in Article 54 (3). Article 54 (4) shall apply in such cases.

(4) In the cases referred to in Paragraph (3), the controller shall inform the data subject in writing within the period referred to in Article 53 (3) of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision would undermine a purpose under Article 54 (3). The controller shall inform the data subject of the right to lodge a complaint with the Commission or, respectively, with the Inspectorate, or to seek a judicial remedy.

(5) The controller shall document the factual or legal reasons on which the decision is based. That information shall be made available to the Commission or, respectively, to the Inspectorate.

Article 56. (New, SG No 17 of 2019) (1) The data subject shall have the right to obtain from the controller the rectification of inaccurate personal data concerning

him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

(2) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her where the processing infringes the provisions of Article 45, 49 or 51 or where the personal data have to be erased for compliance with a legal obligation of the controller.

(3) The controller shall rectify or complete the data under Paragraph (1) or shall erase the data in the cases under Paragraph (2) within the period referred to in Article 53 (3).

(4) The controller shall restrict the processing of the personal data without erasing them where:

1. the accuracy of the personal data is contested by the data subject and this cannot be ascertained, or

2. the personal data must be maintained for the purposes of evidence.

(5) In the cases referred to in Item 1 of Paragraph (4), the controller shall inform the data subject before lifting the restriction of processing.

(6) Rectification, completion, erasure or restriction of the processing of personal data may be refused, taking account of the fundamental rights and legitimate interests of the natural person concerned in the cases referred to in Article 54 (3). Article 54 (4) shall apply in such cases. The controller shall inform the data subject in writing of the refusal and of the reasons for the said refusal within the period referred to in Article 53 (3).

(7) The controller may omit to inform the data subject of the refusal under Paragraph (6) in the cases referred to in Article 54 (3), with Article 54 (4) and (5) applying accordingly.

(8) The controller shall inform the data subject of the right to lodge a complaint with the Commission or, respectively, with the Inspectorate and to seek a judicial remedy.

(9) The controller shall communicate the rectification of inaccurate data to the competent authority from which the said data were received.

(10) Where personal data have been rectified, completed, erased or the processing has been restricted, the controller shall notify the recipient of the said data, and the said recipients shall accordingly rectify, complete, erase or restrict processing of the said data.

Article 57. (New, SG No 17 of 2019) (1) In the cases referred to in Article 54 (3), Article 55 (3) and (4) and Article 56 (6) and (7), the data subject may exercise the rights through the Commission or, respectively, through the Inspectorate. In such cases, the Commission or, respectively, the Inspectorate, shall verify the lawfulness of the refusal.

(2) In the cases referred to in Paragraph (1), the Commission or, respectively, the Inspectorate, shall inform the data subject at least that all necessary verifications or consultations have taken place and of the right of the data subject to seek a judicial remedy.

Article 58. (New, SG No 17 of 2019) The exercise of the rights referred to in Articles 54, 55 and 56, where the personal data are contained in a judicial decision or record or case file prepared in the course of criminal proceedings, shall be without prejudice and may not be contrary to the provisions of the Criminal Procedure Code.



### **Section III**

#### **Data Controller and Processor (New, SG No 17 of 2019)**

Article 59. (New, SG No 17 of 2019) (1) The data controller, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Act. Those measures shall be reviewed and updated where necessary.

(2) Where proportionate in relation to processing activities, the measures referred to in Paragraph (1) shall include the implementation of appropriate data protection policies by the controller.

(3) By measures referred to in Paragraph (1), the controller shall ensure the protection of personal data by design, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks for rights and freedoms of natural persons posed by the processing. The measures must comply with the requirements of Article 45, they shall be planned at the time of the determination of the means for processing of personal data and shall be implemented at the time of the processing itself. Such measures may include pseudonymisation, data minimisation and integrating the necessary safeguards into the processing of personal data.

(4) By measures referred to in Paragraph (1), the controller shall ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation shall apply to the amount of personal data collected, the extent of their processing, the period of the storage and the accessibility. Such measures shall ensure that by default personal data are not made accessible without the intervention of the natural person to an indefinite number of natural persons.

Article 60. (New, SG No 17 of 2019) (1) Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

(2) The joint controllers referred to in Paragraph (1) shall in a transparent manner determine the rights and duties under this Chapter, in particular as regards the exercising of the rights of the data subject and the providing of the information under the procedure of Article 54 by means of joint rules, unless the rights and duties are provided for in Union law or in the legislation of the Republic of Bulgaria. The rules shall designate a contact point for data subjects, and the joint controllers may indicate one of the said controllers to act as a single contact point.

(3) Irrespective of the condition laid down in the rules referred to in Paragraph (1), the data subject may exercise the rights under this Chapter in respect of each of the controllers referred to in Paragraph (1).

Article 61. (New, SG No 17 of 2019) (1) A data controller may entrust processing of personal data on behalf of the said controller only to processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Chapter and ensure the protection of the rights of the data subject.

(2) The processor may not engage another processor for processing without prior specific or general written authorisation of the controller under Paragraph (1). In

the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, and the controller shall have the opportunity to object to such changes.

(3) The processing by the processor shall be governed by a contract or other legal act under Union law or the legislation of the Republic of Bulgaria, that is binding on the processor with regard to the controller referred to in Paragraph (1) and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. The said contract or other legal act shall stipulate, in particular, that the processor:

1. acts only on instructions from the controller;
2. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. assists the controller by any appropriate means to ensure respect for the rights of the data subject;
4. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union law or the law of the Republic of Bulgaria requires storage of the personal data;
5. makes available to the controller all information necessary to demonstrate compliance with this Article;
6. complies with the conditions referred to in Items 1 to 6 and in Paragraph (2) for engaging another processor.

(4) The contract or the other legal act referred to in Paragraph (3) shall be in writing, including in electronic form.

(5) Where a processor determines, in infringement of the rules of this Chapter, the purposes and means of processing, the said processor shall be considered to be a data controller in respect of that processing.

(6) The processor and any person acting under the authority or under the authority of the controller referred to in Paragraph (1) shall not process the said data except on instructions from the controller, unless the conditions and procedure for the processing are provided for in Union law or in the legislation of the Republic of Bulgaria.

Article 62. (New, SG No 17 of 2019) (1) The data controller shall maintain a record of the categories of personal data processing activities which shall contain:

1. the name and contact details of the controller and, where applicable, the joint controllers and the data protection officer;
2. the purposes of the processing of personal data;
3. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
4. a description of the categories of data subject and of the categories of personal data;
5. where applicable, information on whether profile is used;
6. where applicable, the categories of transfers of personal data to a third country or an international organisation;
7. the legal basis for the processing operation, including transfers, for which the personal data are intended;
8. where possible, the envisaged time limits for erasure of the different

categories of data;

9. where possible, a general description of the technical and organisational security measures referred to in Article 66.

(2) The processor shall maintain a record of the categories of personal data processing activities carried out on behalf of a controller, containing:

1. the name and contact details of the processor or processors, of each data controller on behalf of which the processor is acting, and, where applicable, of the data protection officer;

2. the categories of processing of personal data carried out on behalf of each controller;

3. where applicable, transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of the said third country or international organisation;

4. where possible, a general description of the technical and organisational security measures referred to in Article 66.

(3) The records referred to in Paragraphs (1) and (2) shall be in writing, including in electronic form.

(4) The controller and the processor shall make the records available to the Commission or, respectively, to the Inspectorate on request.

Article 63. (New, SG No 17 of 2019) (1) Logs shall be kept in the automated processing systems maintained by the controller and the processor for at least the following processing operations: collection, alteration, consultation, disclosure including transfers, combination and erasure.

(2) The logs of consultation or disclosure of data under Paragraph (1) must make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

(3) The logs referred to in Paragraph (1) shall be used solely for the verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings.

(4) The data controller shall establish appropriate time limits for storage, including archiving of the logs referred to in Paragraph (1).

(5) The controller and the processor shall make the logs referred to in Paragraph (1) available to the Commission or, respectively, to the Inspectorate on request.

Article 64. (New, SG No 17 of 2019) Where a type of processing in particular such using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) The assessment referred to in Paragraph (1) shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Chapter taking into account the rights and legitimate interests of data subjects and other persons concerned.

Article 65. (New, SG No 17 of 2019) (1) The controller or processor shall consult the Commission or, respectively, the Inspectorate, prior to processing which shall form part of a new filing system to be created, where:

1. an impact assessment under Article 64 indicates that the processing would result in a high risk despite the measures taken by the controller to mitigate the risk, or

2. the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

(2) The Commission or, respectively, the Inspectorate, shall be consulted during the preparation of draft laws and draft statutory instruments of secondary legislation containing measures relating to processing.

(3) The Commission shall adopt and publish a list of the processing operations which are subject to mandatory prior consultation under Paragraph (1). The Inspectorate shall apply the list referred to in sentence one accordingly.

(4) The controller shall provide the Commission or, respectively, the Inspectorate, with the data protection impact assessment under Article 64 and, on request, with any other information to allow the Commission or, respectively, the Inspectorate, to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards for the said protection.

(5) Where the Commission or, respectively, the Inspectorate, is of the opinion that the intended processing referred to in Paragraph (1) would infringe the provisions of this Chapter, in particular where the controller has insufficiently identified or mitigated the risk, the Commission or, respectively, the Inspectorate, shall provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor. That period may be extended by a month, taking into account the complexity of the intended processing. The Commission or, respectively, the Inspectorate, shall inform the controller and, where applicable, the processor, of any such extension of the period within up to one month of receipt of the request for consultation together with the reasons for the delay.

(6) The provision of written advice under Paragraph (5) shall be without prejudice to the possibility of the Commission or, respectively, of the Inspectorate, to exercise the powers referred to in Article 80 in respect of the controller or processor.

Article 66. (New, SG No 17 of 2019) (1) The controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks for the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of the categories of personal data referred to in Article 51 (1).

(2) In respect of automated processing, the controller or processor, following an evaluation of the risks, shall implement measures designed to:

1. equipment access control: deny unauthorised persons access to processing equipment used for processing of personal data;

2. data media control: prevent the unauthorised reading, copying, modification or removal of data media;

3. storage control: prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data;

4. user control: prevent the use of automated processing systems by unauthorised persons using data communication equipment;

5. data access control: ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation;

6. communication control: ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment;

7. input control: ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input;

8. transport control: prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media;

9. recovery: ensure that installed systems may, in the case of interruption, be restored;

10. reliability: ensure that the functions of the system perform and that the appearance of faults in the functions is reported;

11. integrity: ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system.

Article 67. (New, SG No 17 of 2019) (1) In the case of a personal data breach which is likely to result in a risk to the rights and freedoms of data subjects, the controller shall notify the Commission or, respectively, the Inspectorate, of the said breach without undue delay but not later than 72 hours after having become aware of the said breach. Where the notification is made after the time limit referred to in sentence one, the said notification shall state reasons for the delay.

(2) The processor shall notify the controller without undue delay but not later than 72 hours after having become aware of a personal data breach.

(3) The notification referred to in Paragraph (1) shall contain at least:

1. a description of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2. the name and contact details of the data protection officer or other contact point where more information can be obtained;

3. a description of the likely consequences of the personal data breach;

4. a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(4) Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(5) The controller shall document any personal data breaches referred to in Paragraph (1), comprising the facts relating to the breach, the effects and the remedial action taken.

(6) Where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State of the European Union, the information referred to in Paragraph (3) shall be communicated to the said controller without undue delay but not later than seven days after the breach has been ascertained.

Article 68. (New, SG No 17 of 2019) (1) Where the personal data security breach referred to in Article 67 (1) is likely to result in a risk to the rights and freedoms of data subjects, the data controller shall notify the data subject as well of the breach within seven days after the breach has been ascertained.

(2) The notification under Paragraph (1) shall describe in clear and plain language the personal data breach and shall contain at least the information and measures referred to in Items 2, 3 and 4 of Article 67 (3).

(3) The data subject shall not be notified of a breach referred to in Paragraph (1) where any of the following conditions are met:

1. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who does not have the right to access the said data, such as encryption;

2. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

3. the notification would involve a disproportionate effort; in such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

(4) Where the controller has not notified the data subject of the personal data security breach referred to in Paragraph (1), the Commission or, respectively, the Inspectorate, having considered the likelihood of the breach resulting in a high risk, may require the controller to notify the data subject.

(5) In the cases referred to in Article 54 (3), the controller may omit to notify the data subject of the breach referred to in Paragraph (1), may notify the said subject after the time limit referred to in Paragraph (1), and may restrict the information referred to in Paragraph (2).

Article 69. (New, SG No 17 of 2019) (1) The data controller shall designate a data protection officer on the basis of his or her professional qualities and, in particular, his or her expert knowledge of personal data protection law and practice and ability to fulfil the tasks referred to in Article 70.

(2) A single data protection officer may be designated for several controllers, taking account of the organisational structure and size of the said controllers.

(3) The controller shall make public by any appropriate means the contact details of the data protection officer and shall notify the Commission under the procedure of Article 25b.

(4) The data protection officers who are designated by the judicial authorities shall not fulfil the tasks referred to in Article 70 when personal data are processed for the purposes referred to in Article 42 (1) by the court, the prosecuting magistracy and the investigating authorities when acting in the judicial capacity .

Article 70. (New, SG No 17 of 2019) (1) The data controller shall ensure that the data protection officer is involved, properly and in a timely manner, in addressing all issues which relate to the protection of personal data.

(2) The controller shall entrust the data protection officer at least with the following tasks:

1. to inform and advise the controller and the employees who carry out processing of the obligations under this Act and in accordance with other statutory requirements for personal data protection;

2. to monitor compliance with this Act and with other statutory requirements

for personal data protection and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

3. to provide advice where requested as regards the data protection impact assessment under Article 64 and monitor the performance of the said assessment;

4. to cooperate with the Commission or, respectively, with the Inspectorate;

5. to act as the contact point for the Commission, including for the purposes of the prior consultation referred to in Article 65, and to consult, where appropriate, the Commission or, respectively, the Inspectorate, with regard to matters concerning personal data processing.

(3) The controller shall provide technical and organisational support to the data protection officer in carrying out the activity, including by providing the necessary resources, access to personal data and processing operations, and to maintain the expert knowledge of the said officer.

Article 71. (New, SG No 17 of 2019) The competent authorities shall put in place appropriate procedures enabling the staff to report, directly and confidentially, any infringements under this Chapter to the competent administrative unit within the structure of the controller or of the Commission, respectively, of the Inspectorate.

#### **Section IV**

#### **Transfers of Personal Data to Third Countries or International Organisations (New, SG No 17 of 2019)**

Article 72. (New, SG No 17 of 2019) (1) A competent authority may transfer personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation provided that the transfer takes place in compliance with this Act and all of the following conditions are fulfilled:

1. the transfer is necessary for the purposes referred to in Article 42 (1);

2. the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 42 (1);

3. where personal data received from another Member State of the European Union are transmitted, that Member State has given its prior authorisation to the transfer in accordance with its national law;

4. where:

(a) the European Commission has adopted a decision to the effect that the third country, territory or one or more specified sectors in the third country concerned, or the international organisation concerned, ensure an adequate level of protection, or

(b) in the absence of a decision under Littera (a), appropriate safeguards have been provided or exist pursuant to Article 74, or

(c) in the absence of a decision under Littera (a) and of appropriate safeguards under Littera (b), the transfer of the personal data is necessary in the cases referred to in Article 75;

5. in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another

competent authority in the Republic of Bulgaria authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

(2) Transfers of personal data without the prior authorisation by another Member State of the European Union in accordance with Item 3 of Paragraph (3) shall be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public order and security of a Member State of the European Union or a third country or to essential interests of a Member State of the European Union and the prior authorisation cannot be obtained in good time. In such cases, the authority of the Member State of the European Union that provided the personal data, which is competent to give prior authorisation under Item 3 of Paragraph (1), shall be informed.

Article 73. (New, SG No 17 of 2019) Where the European Commission repeals, amends or suspend any decision referred to in Item 4 (a) of Article 72 (1), transfer of personal data to the third country, territory or one or more specified sectors in the third country concerned, or the international organisation concerned, may take place under the conditions of Articles 74 and 75.

Article 74. (New, SG No 17 of 2019) (1) In the absence of a decision of the European Commission under Item 4 (a) of Article 72 (1), a transfer of personal data to a third country or an international organisation may take place where:

1. appropriate safeguards with regard to the protection of personal data are provided for in the legislation of the third country or in the statute of the international organisation, or in an international treaty which has entered into force and to which the Republic of Bulgaria is a party, or in another legally binding instrument, or

2. the controller has assessed the circumstances related to the transfer of personal data and has determined that appropriate safeguards exist with regard to the protection of personal data.

(2) The controller shall document the transfer in the cases referred to in Item 2 of Paragraph (1), including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

(3) The controller shall inform the Commission or, respectively, the Inspectorate, of the categories of transfers under Item 2 of Paragraph (1) and, on request, shall make the documentation referred to in Paragraph (2) available to the Commission or, respectively, to the Inspectorate.

Article 75. (New, SG No 17 of 2019) (1) In the absence of a decision of the European Commission under Item 4 (a) of Article 72 (1) or of appropriate safeguards pursuant to Article 74, a transfer of personal data to a third country or an international organisation may take place only if the transfer is necessary:

1. in order to protect the vital interests of the data subject or another person;

2. to safeguard legitimate interests of the data subject, where the legislation of the Republic of Bulgaria so provides;

3. for the prevention of an immediate and serious threat to public order and security of a Member State of the European Union or a third country;

4. in individual cases for the purposes referred to in Article 42 (1), or

5. in an individual case for the establishment, exercise or defence of legal



claims relating to the purposes referred to in Article 42 (1).

(2) Personal data may not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject override the public interest in the transfer under Items 4 and 5 of Paragraph (1).

(3) Any transfer referred to in Paragraph (1) shall be documented and the documentation shall be made available to the Commission or, respectively, to the Inspectorate on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

Article 76. (New, SG No 17 of 2019) (1) In individual and specific cases, a competent authority may, in the absence of the condition referred to in Item 2 of Article 72 (1) and without prejudice to any international treaty, transfer personal data directly to recipients established in third countries only if the other provisions of this Chapter are complied with and all of the following conditions are fulfilled:

1. unless the data are transferred, a task of the transferring competent authority arising from Union law or from the legislation of the Republic of Bulgaria for the purposes referred to in Article 42 (1) cannot be performed, or the performance of the said task would be seriously hindered;

2. the transferring competent authority determines that the fundamental rights and freedoms of the data subject do not override the public interest necessitating the transfer in the case at hand;

3. the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 42 (1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

4. the authority that is competent for the purposes referred to in Article 42 (1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;

5. the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the recipient provided that such processing is necessary.

(2) An international treaty referred to in Paragraph (1) shall be any bilateral or multilateral international agreement in force between Member States of the European Union and third countries in the field of judicial cooperation in criminal matters and police cooperation.

(3) The competent authority transferring the personal data shall document any transfer under Paragraph (1) and shall inform the Commission or, respectively, the Inspectorate, of the said transfer.

Article 77. (New, SG No 17 of 2019) In relation to third countries and international organisations, the Commission shall take appropriate steps to:

1. develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

2. provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

3. engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

4. promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

## **Section V**

### **Supervision of Compliance with Personal Data Protection Rules. Remedies (New, SG No 17 of 2019)**

Article 78. (New, SG No 17 of 2019) (1) Supervision under this Chapter with regard to the processing of personal data for the purposes referred to in Article 42 (1) shall be exercised by the Commission except in the cases referred to in Paragraph (2).

(2) Supervision under this Chapter with regard to the processing of personal data for the purposes referred to in Article 42 (1) by the court, the prosecuting magistracy and the investigating authorities when acting in the judicial capacity shall be exercised by the Inspectorate.

Article 79. (New, SG No 17 of 2019) (1) In exercising supervision under this Chapter, the Commission or, respectively, the Inspectorate, shall perform the following tasks:

1. monitor and enforce the application of the provisions of this Chapter;
2. promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data;
3. raise the awareness of controllers and processors of the obligations;
4. upon request, provide information to any data subject concerning the exercise of the rights and, if necessary, cooperate with the supervisory authorities in other Member States of the European Union to that end;
5. deal with complaints lodged by a data subject under the conditions of Chapter Seven;
6. check the lawfulness of processing in the cases referred to in Article 57 and inform the data subject of the outcome of the check within three months after the infringement has been brought to the attention of the Commission or, respectively, the Inspectorate, or of the reasons why the check has not been carried out;
7. cooperate with other supervisory authorities, including by sharing information, and provide mutual assistance thereto, with a view to ensuring the consistency of application and enforcement of personal data protection rules;
8. conduct investigations in the field of personal data protection, including on the basis of information received from another supervisory authority or other public authority;
9. follow the development of information and communication technologies insofar as they have an impact on the protection of personal data.

(2) In addition to the tasks referred to in Paragraph (1), in exercising supervision under this Chapter the Commission shall furthermore perform the tasks referred to in Article 10 (2) and shall participate in the activities of the European Data Protection Board.

(3) When the tasks referred to in Paragraph (1) are performed, a fee shall not be charged from the data subject and from the data protection officer.

(4) The controller and the processor shall cooperate on request with the Commission or, respectively, with the Inspectorate during the performance of the tasks .

Article 80. (New, SG No 17 of 2019) (1) In exercising supervision under this Chapter, the Commission or, respectively, the Inspectorate, shall have powers:

1. to obtain from the controller or from the processor access to all personal data that are being processed;

2. to obtain from the controller or from the processor all information necessary for the performance of the tasks referred to in Article 79;

3. to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions of this Chapter;

4. to order the controller or processor to bring data processing operations into compliance with the provisions of this Chapter, including to order the rectification, completion or erasure of personal data or restriction of the processing pursuant to Article 56;

5. to impose a temporary or definitive limitation, including a ban, on data processing;

6. to advise the controller and the processor in accordance with the prior consultation procedure referred to in Article 65;

7. to issue, on its own initiative or on request, opinions on draft laws and other statutory instruments, as well as on administrative measures related to the protection of the personal data of natural persons;

8. to issue, on its own initiative or on request, opinions on issues related to the protection of personal data.

(2) In addition to the powers referred to in Paragraph (1), the Commission or, respectively, the Inspectorate, shall furthermore exercise the powers referred to in Item 2 of Article 10a (2) or, respectively, Item 2 of Article 17a (2).

(3) The Commission or, respectively, the Inspectorate, may bring an infringement under this Chapter to the attention of the court.

Article 81. (New, SG No 17 of 2019) (1) The Commission or, respectively, the Inspectorate, shall cooperate with the respective supervisory authorities of the other Member States of the European Union, including by means of exchanging information and making and complying with requests to carry out consultations, inspections and investigations. Requests should contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

(2) The Commission or, respectively, the Inspectorate, shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month of receipt of the request.

(3) The Commission or, respectively, the Inspectorate, may refuse to act on a request under Paragraph (1), stating reasons for the refusal, where:

1. the Commission or, respectively, the Inspectorate, is not competent for the subject-matter of the request or for the measures it is requested to execute, or

2. compliance with the request would infringe the legislation of the Republic of Bulgaria or Union law.

(4) The Commission or, respectively, the Inspectorate, shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request.

(5) The forms of cooperation and mutual assistance between the Commission or, respectively, the Inspectorate, and the supervisory authorities of other Member States of the European Union and the procedures under which such cooperation and assistance are implemented shall be determined by the rules referred to in Article 9 (2)

or, respectively, by the rules referred to in Article 55 (8) of the Judicial System Act.

Article 82. (New, SG No 17 of 2019) (1) In the case of an infringement of the rights under this Chapter, the data subject shall have the remedies and may claim liability for the damage inflicted thereon under the procedure of Chapter Seven.

(2) In the cases referred to in Article 38 (1) and Article 38b (1), the Commission or, respectively, the Inspectorate, shall facilitate the submission of a complaint by a data subject by providing a complaint submission form.

Article 83. (New, SG No 17 of 2019) (1) The data subject shall have the right to mandate a not-for-profit legal person, which has statutory objectives which are in the public interest and is active in the field of protection of the rights and freedoms of natural persons with regard to the protection of their personal data, to lodge a complaint on his or her behalf and to exercise the rights referred to in Article 38 (1) and (6), Article 38b (1), Article 38c (4) and (5) and Article 39 (1) on his or her behalf.

(2) The data subject may not mandate any person referred to in Paragraph (1) to exercise his or her right to receive compensation under Article 39 (2).

## **Chapter Nine**

### **COMPULSORY ADMINISTRATIVE MEASURES. ADMINISTRATIVE PENALTY PROVISIONS (NEW, SG No 17 OF 2019)**

Article 84. (New, SG No 17 of 2019) The measures referred to in Items (a) to (g) and (j) of Article 58 (2) of Regulation (EU) 2016/679 and the measures referred to in Items 3, 4 and 5 of Article 80 (1) shall be compulsory administrative measures within the meaning of the Administrative Violations and Sanctions Act.

(2) The measures referred to in Paragraph (1) shall be applied by a decision of the Commission or, respectively, of the Inspectorate, which shall be appealable under the procedure of the Administrative Procedure Code within 14 days of receipt of the said decision.

Article 85. (New, SG No 17 of 2019) (1) For violations under Article 25c of the data controller or data processor shall be imposed a fine or pecuniary sanction in the amounts under Article 83, Paragraph (4) of Regulation (EU) 2016/679.

(2) (Amend. - SG 11/23, in force from 04.05.2023) For violations under Art. 12a, Para. 1, Art. 25d, Art. 25f, Para. 2, Art. 25g, Para. 1 and 2, Art. 25h, Para. 1 and 2, Art. 25i, Art. 25k and Art. 25n, the administrator or the personal data processor shall be imposed a fine or proprietary sanction in the amounts under Art. 83, Para. 5 of Regulation (EU) 2016/679.

(3) For violations under Article 45, Article 49, Article 51, Articles 53-56 and Article 80 (1), Items 1 and 2, the data controller or the data processor shall be imposed a fine or pecuniary sanction in the amounts under Article 83, Paragraph (5) of Regulation (EU) 2016/679.

(4) For violations under Article 59, Paragraphs (3) and (4), Articles 62 and 64 – 70, the data controller or the data processor shall be imposed a fine or a pecuniary sanction in the amounts under Article 83, Paragraph (4) of Regulation (EU) 2016/679.

(5) For non-compliance of an enforced decision under Article 84, Paragraph (2), which has applied compulsory administrative measures under Article 80, Paragraph (1), Items 4 and 5, the data controller or the data processor shall be subject

to a fine or pecuniary sanction in the amounts under Article 83, Paragraph (5) of Regulation (EU) 2016/679.

(6) The amounts, provided for in Para. 1-5, administrative penalties shall be determined according to the indication criteria of Art. 83, Para. 2 of Regulation (EU) 2016/679 and their BGN equivalent shall be imposed.

(7) (New - SG 11/23, in force from 04.05.2023) For a violation under Para. 2, an administrative measure may be imposed and/or coercive measure under Art. 58, Para. 2, letters "a" - "h" and "j" of Regulation (EU) 2016/679.

Article 86. (New, SG No 17 of 2019) (1) For other violations under this Act, a data controller or data processor shall be liable to a fine or a pecuniary sanction of up to BGN 5,000.

(2) For a repeated violation under Paragraph (1), shall be imposed a fine or a pecuniary sanction in double of the amount, initially imposed.

Article 87. (New, SG No 17 of 2019) (1) In cases other than those referred to in Article 38, Paragraph (1), the ascertainment of the infringements of Regulation (EU) 2016/679 or of this Act, the issue, appellate review and execution of penalty decrees shall follow the procedure of the Administrative Infringement and Penalties Act.

(2) The written statements ascertaining the administrative infringements shall be drawn up by a member of the Commission or by officials empowered by the Commission or, respectively, by persons empowered by an order of the Inspector General.

(3) The penalty decrees shall be issued by the Chairperson of the Commission or, respectively, by the Inspector General or by inspectors empowered.

(4) The pecuniary sanctions and fines under enforceable decisions referred to in Article 38 Paragraph (3) and penalty decrees shall be collected under the procedure of the Tax and Social Security Procedure Code.

(5) The amounts, collected from property sanctions and fines, imposed by the Commission shall be transferred into the Commission's budget.

(6) The collected amounts of pecuniary sanctions and fines imposed by the Inspectorate shall be transferred into the budget of the judiciary.

### **Supplementary provisions**

§ 1. (Amended, SG No 17 of 2019) Within the meaning of this Act:

1. "Personal data" shall be the term defined in Article 4 Paragraph 1 of Regulation (EU) 2016/679.

2. "Controller", with the exception of the controller under Chapter Eight, shall be the term defined in Article 4 Paragraph 7 of Regulation (EU) 2016/679.

3. "Processor" shall be the term defined in Article 4 Paragraph 8 of Regulation (EU) 2016/679.

4. "Processing" shall be the term defined in Article 4 Paragraph 2 of Regulation (EU) 2016/679.

5. "Restriction of processing" shall be the term defined in Article 4 Paragraph 2 of Regulation (EU) 2016/679.

6. "Profiling" shall be the term defined in Article 4 Paragraph 4 of Regulation (EU) 2016/679.

7. “Pseudonymisation” shall be the term defined in Article 4 Paragraph 5 of Regulation (EU) 2016/679.

8. “Filing system” shall be the term defined in Article 4 Paragraph 6 of Regulation (EU) 2016/679.

9. “Recipient” shall be the term defined in Article 4 Paragraph 9 of Regulation (EU) 2016/679. Any central or local government authority, as well as any entity whose core activity involves the spending of public funds, which may receive personal data within the framework of a particular investigation in accordance with a law, shall not be regarded as recipients within the meaning of Chapter Eight. The processing of personal data by such authorities or entities shall comply with the applicable data protection rules in accordance with the purposes of the processing.

10. “Personal data breach” shall be the term defined in Article 4 Paragraph 12 of Regulation (EU) 2016/679.

11. “Genetic data” shall be the term defined in Article 4 Paragraph 13 of Regulation (EU) 2016/679.

12. “Biometric data” shall be the term defined in Article 4 Paragraph 14 of Regulation (EU) 2016/679.

13. “Data concerning health” shall be the term defined in Article 4 Paragraph 15 of Regulation (EU) 2016/679.

14. “International organisation” shall be the term defined in Article 4 Paragraph 26 of Regulation (EU) 2016/679.

15. Large-scale (processing operations) shall be monitoring and/or processing of personal data of a significant or unlimited number of data subjects or amount of personal data, where the core activities of the controller or the processor, including the means by which these activities are carried out, consist of such operations.

16. “Risk” shall be the possibility of the data subject suffering a material or non-material damage under specified conditions, assessed in terms of the severity and probability .

17. “Public authority” shall be a central or local government authority, as well as an entity whose core activity involves the spending of public funds.

18. “Erasure” shall be the irrecoverable deletion of information from the medium concerned.

19. “Destruction” shall be the irrecoverable physical disintegration of the tangible data medium.

20. An infringement shall be “repeated” if committed within one year after the decision of the Commission or the penalty decree, whereby the infringer was penalised for an infringement of the same time, became enforceable.

§ 1a. (New, SG No 91 of 2006, amended, SG No 17 of 2019) This Act lays down implementing measures for Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1 of 4 May 2016) and transposes the requirements of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119/89 of 4 May 2016).

## Transitional and Final Provisions

§ 2. (1) The Council of Ministers shall make a proposal for the Chairperson and members of the Commission for Personal Data Protection before the National Assembly within one month of the entry into force of this Act.

(2) The National Assembly shall elect the Chairperson and members of the of the Commission for Personal Data Protection within 14 days of the proposal pursuant entry of the motion under Paragraph (1).

(3) Within 3 months from its election the Commission for Personal Data Protection shall adopt and promulgate in the State Gazette the regulations under Article 9, Paragraph (2).

(4) The Council of Ministers shall provide the property and financial resources necessary for the commencement of work of the Commission within one month of the entry into force of the resolution of the National Assembly referred to in Paragraph (2).

§ 3. (1) The entities or individuals maintaining registers of personal data at the time of entry into force of this Act shall bring the said filing systems into compliance with the requirements of the Act and shall notify the Commission within six months of the entry into force of the rules referred to in Article 9 (2).

(2) The Commission shall carry out preliminary inspections opinions, shall register or shall refuse to register as controllers persons who or which maintain registers by the moment of entry into force of the Act, as well as the registers kept by them within 3 months from the receipt of the application under Paragraph (1).

(3) The decisions of the Commission refusing registration shall be appealable before the Supreme Administrative Court within 14 days.

(4) Upon the entry into effect of the decision of the Commission refusing registration or of the judgment of the Supreme Administrative Court upholding the refusal of the Commission, the person who or which unlawfully keeps a filing system shall be obliged to destroy personal data contained in the filing system or, with the consent of the Commission, to transfer the data to another controller who or which has registered the filing system and processes personal data for the same purposes.

(5) The Commission shall exercise control over the fulfilment of the obligation under Paragraph (4).

(6) The controller referred to in Article 3 (1) shall be obliged to publish the information covered under Article 22 (1) in the bulletin of the Commission for Personal Data Protection within three months of the registration.

§ 4. The Access to Public Information Act (*State Gazette* No 55 of 2000) shall be amended as follows:

1. In Article 2 Paragraph (3), the words “personal information” shall be replaced by “personal data”.

2. In § 1, Item 2 shall be amended to read as follows:

“2. ‘Personal data’ shall be information on an individual disclosing his physical, psychological, mental, marital, economic, cultural or public identity.”

§ 5. This Act shall enter into force as from 1 January 2002.

-----  
The Act was adopted by the 39th National Assembly on December 21, 2001 and was affixed with the official seal of the National Assembly.

**Transitional and Final Provisions**  
**TO THE LAW ON PRIVATE ENFORCEMENT AGENTS**  
(PROMULGATED, SG No 43 OF 2005, IN FORCE AS FROM  
1 SEPTEMBER 2005)

§ 23. This Act shall enter into force as from 1 September 2005.

**Transitional and Final Provisions**  
**TO THE ACT FOR THE AMENDMENT AND SUPPLEMENT OF THE**  
**PERSONAL DATA PROTECTION ACT**  
(PROMULGATED, SG No 103 OF 2005, AMENDED, SG No 91 OF 2006)

§ 50. The provision of § 38 with regard to Article 36 [of the Personal Data Protection Act] shall apply until the entry into force of the Treaty concerning the Accession of the Republic of Bulgaria to the European Union.

§ 51. (Amended, SG No 91 of 2006) The provisions of § 1 with regard to Item 3 of Article 1 (4), Item 1 (c) of § 8 with regard to Item 9 of Article 10 (1), § 39 with regard to Article 36a, § 40 with regard to Article 36b, and Item 5 of § 48 with regard to Item 14 of the Supplementary Provision [of the Personal Data Protection Act] shall enter into force as from the date of entry into force of the Treaty concerning the Accession of the Republic of Bulgaria to the European Union.

§ 52. Within three months of the entry into force of this Act, the Commission for Personal Data Protection shall adopt the Ethical Code referred to in Article 10 (4) and the ordinance referred to in Article 23 (5) [of the Personal Data Protection Act].

**Transitional and Final Provisions**  
**TO THE ADMINISTRATIVE PROCEDURE CODE**  
(PROMULGATED, SG No 30 OF 2006, IN FORCE AS FROM  
12 JULY 2006)

§ 142. This Code shall enter into force three months after the promulgation in the *State Gazette* with the exception of

1. Title Three, Item 1 of § 2 and Item 2 of § 2 (with regard to the repeal of Chapter Three, Section II “Appeal Before the Court” [of the Administrative Procedure Act]), Items 1 and 2 of § 9, Items 1 and 2 of § 11, § 15, Items 1 and 2 of § 44, Item 1 of § 51, Item 1 of § 53, Item 1 of § 61, Item 3 of § 66, Items 1 to 3 of § 76, § 78, § 79, Item 1 of § 83, Items 1 and 2 of § 84, Items 1 to 4 of § 89, Item 1 of § 101, Item 1 of § 102, § 107, Items 1 and 2 of § 117, § 125, Items 1 and 2 of § 128, Item 2 of § 132 and Item 1 of § 136, as well as § 34, Item 2 of § 35, Item 2 of § 43, Item 1 of § 62, Items 2 and 4 of § 66, Item 2 of § 97, and Item 1 of § 125 (with regard to the replacement of the word “district” by “administrative” and the replacement of the words “the Sofia City Court” by “the Sofia City Administrative Court”), which shall enter into force as from 1 March 2007;

2. § 120, which shall enter into force as from 1 January 2007;

3. § 3, which shall enter into force as from the day of promulgation of this Code in the *State Gazette*.



**Transitional and Final Provisions**  
**TO THE ACT FOR THE AMENDMENT AND SUPPLEMENT OF THE**  
**PERSONAL DATA PROTECTION ACT**  
(PROMULGATED, SG No 91 OF 2006)

§ 31. The provision of § 6 with regard to Article 6 (2) [of the Personal Data Protection Act] shall enter into force as from 1 January 2007.

§ 32. Within two months of the entry into force of this Act, the Commission for Personal Data Protection shall adopt the instruction referred to in Article 12 (9) [of the Personal Data Protection Act].

§ 33. Within three months of the entry into force of this Act, the controllers who or which are subject to registration shall submit an application for registration.

**Transitional and Final Provisions**  
**TO THE LAW ON THE NATIONAL ARCHIVE FUNDS**  
(PROMULGATED, SG No 57 OF 2007, IN FORCE AS FROM  
13 JULY 2007)

§ 23. This Act shall enter into force as from the day of promulgation in the *State Gazette*.

**Transitional and Final Provisions**  
**TO THE ACT FOR THE AMENDMENT AND SUPPLEMENT OF THE**  
**CONFLICT OF INTEREST PREVENTION AND DISCLOSURE ACT**  
(PROMULGATED, SG No 97 OF 2010, IN FORCE AS FROM  
10 DECEMBER 2010)

§ 61. This Act shall enter into force as from the day of promulgation in the *State Gazette* with the exception of:

1. § 11 with regard to Articles 22a to 22e [of the Conflict of Interest Prevention and Ascertainment Act], which shall enter into force as from 1 January 2011;

2. § 7, § 8, § 9, § 11 with regard to Articles 22f to 22i [of the Conflict of Interest Prevention and Disclosure Act] and § 12, § 13, § 14, § 15, § 16, § 17, § 18, § 19, § 20, § 21, § 22 and § 23, which shall enter into force as from 1 April 2011.

**Supplementary Provisions**  
**TO THE ACT FOR THE AMENDMENT AND SUPPLEMENT OF THE**  
**PERSONAL DATA PROTECTION ACT**  
(PROMULGATED, SG No 81 OF 2011)

§ 15. This Act transposes the requirements of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350/60 of 30 December 2008).

**Transitional and Final Provisions**  
**TO THE ACT FOR THE AMENDMENT AND SUPPLEMENT OF THE**  
**ELECTRONIC COMMUNICATIONS ACT**  
(PROMULGATED, SG No 105 OF 2011, IN FORCE AS FROM  
29 DECEMBER 2011)

§ 220. This Act shall enter into force as from the day of promulgation in the *State Gazette*.

**Transitional and Final Provisions**  
**TO THE PUBLIC FINANCE ACT**  
(PROMULGATED, SG No 15 OF 2013, IN FORCE AS FROM  
1 JANUARY 2014)

§ 123. This Act shall enter into force as from 1 January 2014 with the exception of § 115, which shall enter into force as from 1 January 2013, and § 18, § 114, § 120, § 121 and § 122, which shall enter into force as from 1 February 2013.

**Transitional and Final Provisions**  
**TO THE ACT FOR THE AMENDMENT AND SUPPLEMENT OF THE**  
**MINISTRY OF INTERIOR ACT**  
(PROMULGATED, SG No 81 OF 2016, IN FORCE AS FROM  
1 JANUARY 2017)

§ 102. This Act shall enter into force as from 1 January 2017 with the exception of:

1. § 6 to 8, Items 1, 2 and 4 of § 12, § 13, § 14, § 18 to 20, § 23, § 26 to 31, Items 1 and 4 of § 32, § 33 to 39, § 41 to 48, § 49 with regard to sentence one of Article 187 (3) [of the Ministry of Interior Act], § 50 to 59, § 61 to 65, § 81 to 85, Items 4 and 5 of § 86, Item 3 of § 87, Item 1 of § 90, Items 2 and 3 of § 91, § 92, § 93 and § 97 to 101, which shall enter into force as from the day of promulgation of the Act in the *State Gazette*;

2. Items 2 and 3 of § 32, § 49 with regard to new sentence two of Article 187 (3) [of the Ministry of Interior Act], § 69 to 72, § 76 with regard to the persons referred to in § 70, § 78 with regard to the officers referred to in § 69 and § 70, § 79 with regard to the officers referred to in § 69 and § 70, Item 1 of § 91 and § 94, which shall enter into force as from 1 February 2017.

**Transitional and Final Provisions**  
**TO THE ACT FOR THE AMENDMENT AND SUPPLEMENT OF THE**  
**ACT RESTRICTING ADMINISTRATIVE REGULATION AND**  
**ADMINISTRATIVE CONTROL OVER ECONOMIC ACTIVITY**  
(PROMULGATED, SG No 103 OF 2017, IN FORCE AS FROM  
1 JANUARY 2018)

§ 68. This Act shall enter into force as from 1 January 2018.

**Transitional and Final Provisions**  
**TO THE ACT FOR THE AMENDMENT AND SUPPLEMENT OF THE**  
**PERSONAL DATA PROTECTION ACT**  
(PROMULGATED, SG No 17 OF 2019)

§ 44. (1) Any proceedings for infringements of the [Personal Data Protection] Act which have been initiated prior to 25 May 2018 and which are not completed by the entry into force of this Act shall be completed under the hitherto effective procedure.

(2) Any infringements of the [Personal Data Protection] Act and of Regulation (EU) 2016/679, which have been committed prior to the entry into force of this Act, shall be brought to the attention of the Commission under Article 38 [of the Data Protection Act] within one year after having become aware of the infringement but not later than five years after the infringement.

§ 45. The automated processing systems used by the competent authorities under Article 42 (4) [of the Personal Data Protection Act] for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public order and security, which have been established prior to 6 May 2016, shall be brought in compliance with Article 63 (1) [of the Personal Data Protection Act] by 6 May 2023.

.....  
§ 120. The Commission for Personal Data Protection shall adopt the ordinances referred to in Article 14 (5) and (6) and in Article 14a (3) [of the Personal Data Protection Act] within one year of the entry into force of this Act.

**Relevant acts of European Union law**

**Directives:**

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 12 JULY 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications)

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (**Repealed**)

**Regulations:**

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

REGULATION (EEC) No 2380/74 of the Council of 17 September 1974 adopting provisions for the dissemination of information relating to research programmes for the European Economic Community

**Decisions:**

COUNCIL FRAMEWORK DECISION 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Repealed)

COMMISSION DECISION of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (notified under document C(2001) 1539)

COMMISSION DECISION of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document C(2000) 2304) (2000/518/EC)